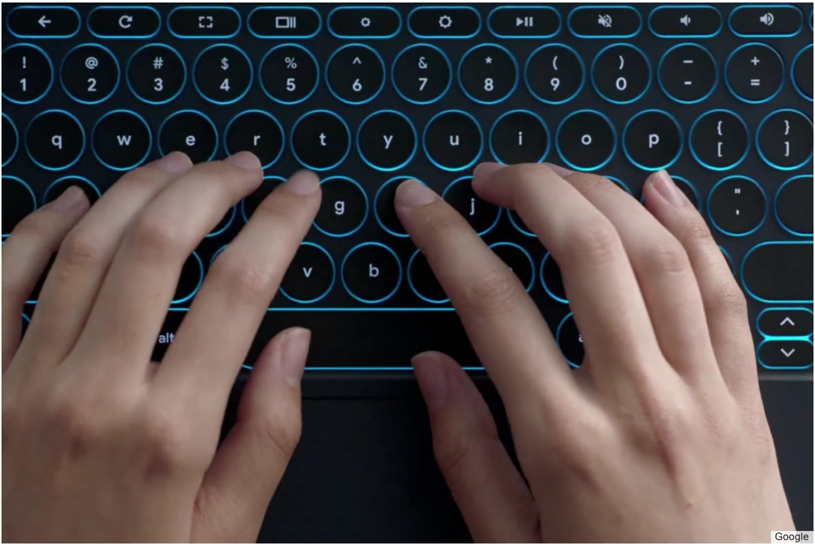
FEATURE

What is a keylogger? How attackers can monitor everything you type

Keystroke logging software is one of the oldest forms of malware, dating back to typewriters. It's still popular and often used as part of larger cyber attacks.

By Dan Swinhoe
Editor, CSO | DEC 11, 2018 3:34 AM PST

cisco SecureX
Get more horsepower out of your cybersecurity investments
Learn how



Google

Keylogger definition

Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

[Get inside the mind of a hacker, learn their motives and their malware. | Sign up for CSO newsletters!]

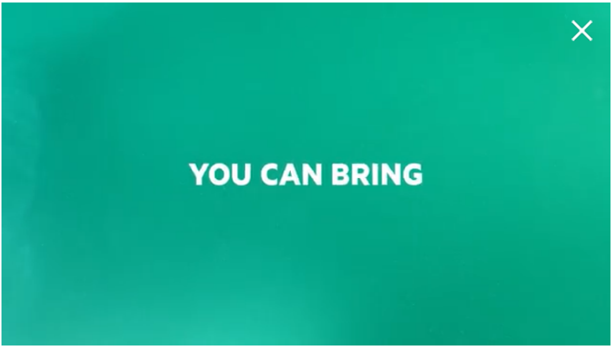
Criminals use keyloggers to steal personal or financial information such as banking details, which they can then sell or use for profit. However, they also have legitimate uses within businesses to troubleshoot, improve user experience, or monitor employees. Law enforcement and intelligence agencies also uses keylogging for surveillance purposes.

Content Continues Below

How do keyloggers work?

Keyloggers collect information and send it back to a third party – whether that is a criminal, law enforcement or IT department. “Keyloggers are software programs that leverage algorithms that monitor keyboard strokes through pattern recognition and other techniques,” explains Tom Bain, vice president security strategy at Morphisec.

The amount of information collected by keylogger software can vary. The most basic forms may only collect the information typed into a single website or application. More sophisticated ones may record everything you type no matter the application, including information you copy and paste. Some variants of keyloggers – especially those targeting mobile devices – go further and record information such as calls (both call history and the audio), information from messaging applications, GPS location, screen grabs, and even microphone and camera capture.



Keyloggers can hardware- or software-based. Hardware-based ones can simply nestle between the keyboard connector and the computer’s port. Software-based ones can be whole applications or tools knowingly used or downloaded, or [malware](#) unknowingly infecting a device.

Data captured by keyloggers can be sent back to attackers via email or uploading log data to predefined websites, databases, or FTP servers. If the keylogger comes bundled within a large attack, actors might simply remotely log into a machine to download keystroke data.

Content Continues Below

How hackers use keyloggers

The first keyloggers were used by the Soviet Union in [the 1970s](#) to monitor IBM electric typewriters used at embassies based in Moscow. They would record what was typed and send the information back to Soviet intelligence via radio signals.

RECOMMENDED WHITEPAPERS

[Deloitte + Google Cloud: Future of the SOC](#)

[Redefining Security Analytics with Chronicle](#)

[Case Study: Global healthcare industry leader](#)

Today spyware such as keystroke loggers are a common part of the cyber-criminal toolset to capture financial information such as banking and credit card details, personal information such as emails and password or names and addresses, or sensitive business information around processes or intellectual property. They may sell that information or use it as part of a larger attack depending on what was gathered and their motives.

Content Continues Below

BrandPost Sponsored by AWS
3 use cases for machine learning you probably haven't thought of
As organizations gain more experience deploying machine learning (ML) and artificial intelligence (AI) across different parts of the business, they're discovering new and interesting ways to use...

"These programs can be used to steal information like passwords, [PII [personally identifiable information]], and other critical information related to individuals and organizations," explains Bain. "For example, if a keylogger is able to monitor the keystrokes of a database super admin within a large organization, they can gain access to things like laptops and servers that can ultimately expose large volumes of data they can monetize."

Keyloggers in the workplace

There is also a large but ethically questionable market for spyware — legal keylogging apps being used by people to spy on their family, friends or partners. This is legal if the one downloading the spyware owns the device or the user knows, but this can often stray into stalking territory. Legal spyware apps that collect information on workers can be lax on security. For example, spyware provider mSpy has suffered at least two data breaches.

Content Continues Below

Sometimes called corporate keylogging, such monitoring software can useful in testing, debugging and user experience. “In an above-board corporate environment, keyloggers are also used to track the activity of users for IT security and regulatory compliance,” says Simon Sharp, international vice president at ObserveIT. “Keylogger records can be used to help administrators investigate system failures and establish what the context around why a breach occurred; an administrator can instantly establish who entered a particular word or value associated with the incident under investigation and thereby understand who violated a policy, when and why.”

IT can use keystroke data to help identify and fix user issues, assist with security and compliance efforts, and possibly provide additional forensic information in the wake of a security incident. They can also be used to flag potential insider threats, monitor employee productivity, or ensure corporate IT assets are only being used for work purposes.

Content Continues Below

SponsoredPost Sponsored by KPMG
Gaining Maximum Value from the Cloud
Organizations Could Cut Back on Cloud-Based Resources with Better Visibility

Windows 10 comes pre-loaded with its own type of keylogger for telemetry purposes. Grammerly – a popular spelling and grammar tool – has been described as “a keylogger with useful features” due to the fact it records what the user types while it is activated.

It is important, however, to remember that you must notify employees if they are being monitored in such a way. Failure to do so could break laws around employee privacy. Any collected keylog data should be encrypted.

How keyloggers infect devices

Keyloggers can be placed on machines in a number of different ways.

Physical loggers require a person to be physically present to be placed on a machine, meaning such attacks are harder (but not impossible) to achieve, and more likely to come from an insider threat. Wireless keyboards can also be snooped on remotely.

Last year hundreds of models of HP laptops were shipped with keylogging code present in its touchpad drivers. The logging was disabled by default and was part of a debug tool left in by one of the company's suppliers.

Content Continues Below

Show notifications

Software-based keyloggers are far more common and have multiple routes for entry. Infected domains are a common attack method. In October, online office suite Zoho saw its .com and .eu domains suspended after serving users keylogging malware. Thousands of Wordpress sites have also been previously infected with keyloggers via fake Google Analytics scripts.

Malware-infected apps are also an issue. Google recently removed 145 apps from the Play Store that contained keylogging malware. As with many types of malware, loggers are often included in phishing emails containing malicious links. A new version of the HawkEye keylogger, for example, was spread via a spam email campaign bearing infected Word documents. Some variants, such as Fauxspersky, can spread through infected USB drives.

Content Continues Below

"The biggest change in keyloggers has been the addition of evasive techniques that allow keylogging to slip past other detection mechanisms, such as antivirus," says Bain. "There are multiple ways that attackers are loading keylogging techniques into adware, which are commonly not whitelisted. When this happens, the adware is allowed to run or isn't flagged, and subsequently not investigated because it's meeting the detection criteria for many detection engines."

Keyloggers often come bundled with other malware as part of a wider attack. Many keyloggers now come with ransomware, cryptocurrency mining or botnet code attached that can be activated at the attacker's discretion.

Content Continues Below

Some universities have suffered incidents due to keyloggers. Nearly 2,000 students at the University of California Irvine had their personal and health information stolen after computers in the student health center were compromised. Last year at the University of Iowa, a student was arrested by the FBI for computer fraud after using a keylogger to gain advance copies of exams and change grades. In 2016 a student at the Singapore Management University used a USB hardware keylogger to gain the user IDs and passwords of two professors to delete the test scripts for an example and force a retake.

6 best practices for detecting and removing keyloggers

The advice below represents what's generally considered as the most effective steps to take to minimize the impact of unwanted keyloggers.

Content Continues Below

1. Monitor resource allocation, processes and data

Observing resource allocation and background process on machines, as well as data being transmitted from the device outside the organization can help identify if a keylogger is present. Keyloggers usually need root access to the machine, which can also be a telltale sign of a keylogger infection.

2. Keep antivirus and anti-rootkit protection up to date

As keyloggers often come bundled with other forms of malware, discovering keylogger malware might be an indicator of a wider attack or infection. Up-to-date antivirus protection and anti-rootkit protectors will remove known keylogger malware, according to Jeff Wichman, practice director for Optiv Security, but may warrant further investigation to determine whether the keylogger was just one component of a larger attack.

Content Continues Below

3. Use anti-keylogger software

Dedicated anti-logger software is designed to encrypt keystrokes as well as scan for and remove known loggers and flag unusual keylogging-like behavior on the machine. Blocking root access for unauthorized applications and blacklisting known spyware apps will also help.

4. Consider virtual onscreen keyboards

Virtual onscreen keyboards reduce the chance of being keylogged as they input information in a different way to physical keyboards. This might impact user productivity, isn't foolproof against all kinds of keystroke monitoring software, and doesn't eliminate the cause of the problem.

Content Continues Below

5. Disable self-running files on external devices

Disabling self-running files on externally connected devices such as USBs and restricting copying of files to and from external to computers may also reduce the possibility of infection.

6. Have a strong password policy

"While checking task managers for unknown or suspicious installations, and recognizing odd occurrences such as keys pausing or not displaying on screen when typing can help individuals detect keyloggers in certain cases," advises Bain, "the best way for organizations to stay safe is to ensure that their password policy is multi-faceted, and that two-factor authentication is implemented across company accounts and devices. It's important to never assume that the average antivirus technology is enough."

Content Continues Below

More on malware

- **What is malware? Viruses, worms, trojans, and beyond**
- **Malware detection in 9 easy steps**
- **How to detect and prevent crypto mining malware**
- **8 types of malware and how to recognize them**
- **Infected with malware? Check your Windows registry**

Next read this

- *8 top open source intelligence tools*
- *How to rob a bank: A social engineering walkthrough*
- *10 common cloud security mistakes that put your data at risk*
- *12 cheap or free cybersecurity training resources*
- *11 types of hackers and how they will harm you*
- *Securing Microsoft Teams: The options are limited*
- *What is security's role in digital transformation?/a>*

Related: Security Malware

Dan Swinhoe is UK Editor of CSO Online

Follow

Copyright © 2018 IDG Communications, Inc.

The 10 most powerful cybersecurity companies

You May Also Like

Recommended by Outbrain

A history of ransomware: The motives and methods behind these evolving attacks

What is identity theft? How to prevent and report it

Shaking off old public sector security perceptions at L&Q Group

CIOs say security must adapt to permanent work-from-home

What it takes to be a transformational CISO

The biggest data breach fines, penalties and settlements so far

Uber breach case a ‘watershed moment’ for...

Australian government doubles down on...

Azure Security Benchmark v2: What you need to know

Homomorphic encryption tools find their niche

4 ways employee home networks and smart devices change your threat model

SPONSORED LINKS

Join the IDG TECH(talk) Community, an exclusive online network where IT experts find resources to enhance their knowledge and career.

Software defines your networks. NETSCOUT defines your visibility. See it all.

Digital Transformation wasn’t supposed to happen this way. You need visibility to gain control. Take control with NETSCOUT .

dtSearch® instantly searches terabytes of files, emails, databases, web data. See site for hundreds of reviews; enterprise & developer evaluations

Copyright © 2020 IDG Communications, Inc.